NETWORK MANAGEMENT ASSIGNMENT PART 2

MAGUN SINGH

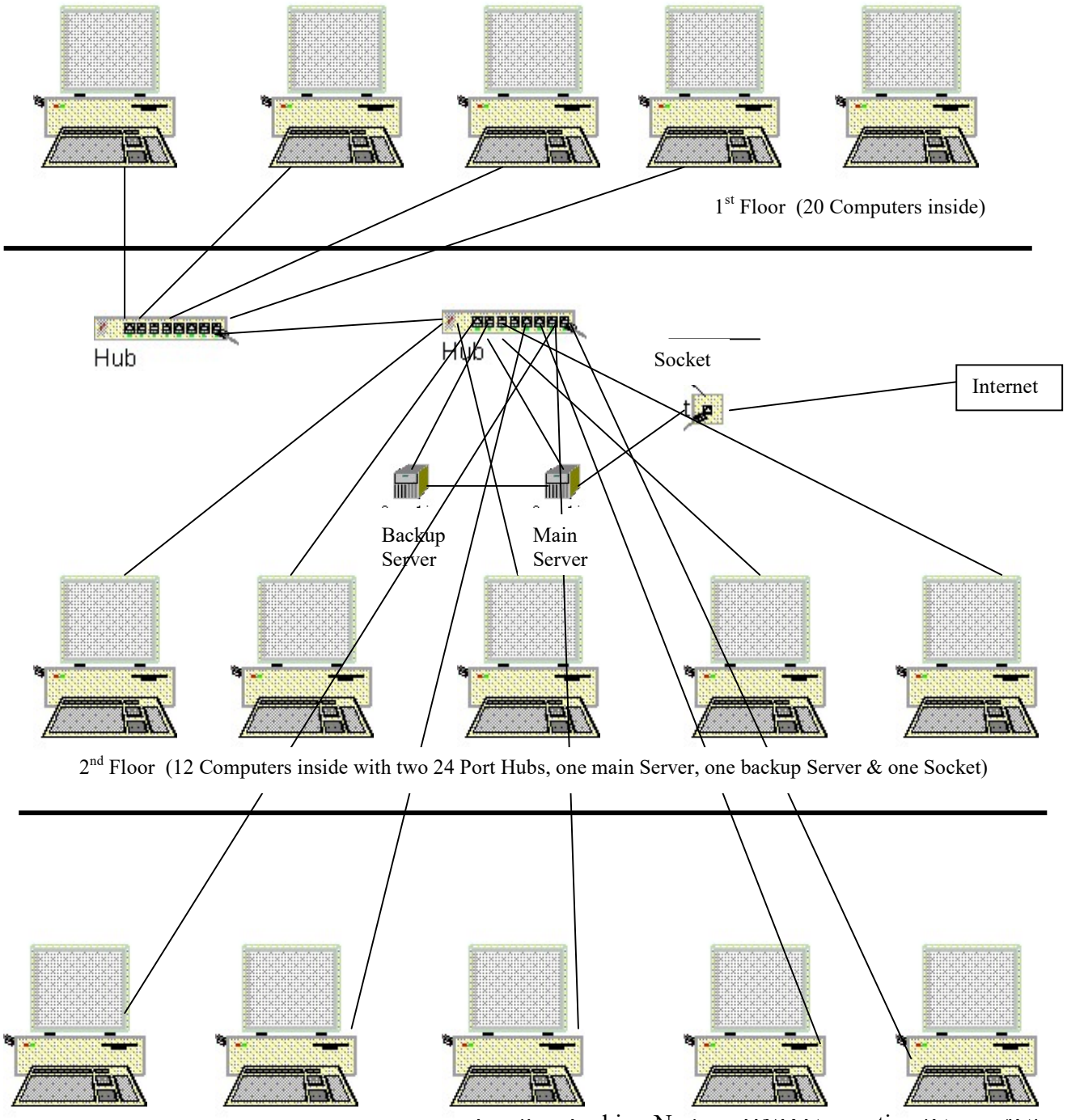
C3 - CHRISTCHURCH COMPUTING COMPANY

BY JONATHAN ERSKINE-NARTEY

Contents

Plan for C3 - Christchurch Computing Company

A plan (roughly to give an idea)



C3 - Christchurch Computing Company

If you are looking at all networks on 3 different sites, it is pretty obvious that we should choose LAN 1OObaseTX. We are assuming that Site 2 has Network cards capable of running at 1OOMB. Also it makes sense that both Site 1 and Site 3 should be re-cabled to the RJ-45 (Cat 5) cabling standard. As done in my previous Assignment (Multimedia Epics Inc.). We are assuming that Site 2 is already cabled up to Cat 5 standard so all three Sites are lOObaseTX?

The network operating system that I have decided to use for this company is both Microsoft NT Server and Workstation, the reason for this preference is basically flexibility adaptability and reliability. Flexibility in the sense that it works on most hardware adaptability due to the fact it can connect to different operating systems i.e. Linux, Novel and reliability because it is the most widely used operating system in the world.

Based on our assumptions and relevant changes for site 1 and 3 we would purchase the relevant network cards to replace the existing ones as all networks will therefore be running at 1OOMBs, (total of 25 network cards), purchasing these cards is beneficial, as we will be increasing both networks speeds to run 10 times quicker and also when we decide to upgrade the existing hardware we can exclude the cost of network cards as these can be taken out and put in our new machines.

An alternative would be in theory just to have a 10MB running at all sites and leave all the sites as they were. But a recommendation would be definitely to have site 1 rewired, as BNC cabling is susceptible to breakages and in some cases interference.

Site 1 already has a Microsoft operating system (Windows 95) on the client, there are three approaches that we can apply to site 1 depending on budget, the following easiest options are:

- Option No 1: Would be to just to replace the Novell server with a Windows NT Server if the Novell Server hardware meet's the NT server specifications (such as the Processor speed, memory - RAM, storage, hardware, etc.). Then we could use the same machine otherwise we should purchase a relevant machine. The client would still be running Windows 95.

- Option No 2 is the full-blown conversion, which is to upgrade the existing Novell Server to a NT server or purchase a new one, if hardware does not meet NT specifications, and then hardware permitting on the clients to upgrade the Windows 95 operating system to Windows NT workstation.

- Option No 3: We are proposing to deploy Microsoft Windows NT Workstation Server through out the company's environment site 1 and 2 would have no problem in transition to this state as site 2 is already our preferred solution and site 1 which currently uses Windows 95 has the same look and feel fortunate for us there are only 5 workstations at site 3 and it appears to be the smallest site in the company this would be our only problem, in retraining the users to use the new software. To be honest most people nowadays have computers at home and we are assuming majority of them uses windows so it should not be that bigger job.

Site 3 we would need to access the current hardware and if it can cope install Windows NT server on the Linux server and installing Windows NT Workstations on the 5 Linux workstations. I strongly recommend that since this is a small site we should purchase new hardware for everything bearing in mind the hardware purchased can be reused in the new installations.

Assumption on all NT servers at Sites 1, 2 & 3, we will have Microsoft sequel Server running. Also that the existing databases at each site have been converted and changed to a SQL database.

Assumptions for C3 - Christchurch Computing Company

The following assumptions that have been made while going through the configurations of a network system for C3 - Christchurch Computing Company are:

- They are used existing 37 Intel (PC) based computers and 5 printers on the premises.
- They have the sockets to use the ISDN connection.
- They already have a 2Mbps leased line connection.
- They have necessary suitable routers
- They already have a supply of UPS in case of power failure.
- All PCs have Internet connections and modems to go with it.
- Assuming that the company has suspended ceilings in their offices on each floor to allow for the cabling.
- I have decided to put 20 computers on Site No. 1, 12 computers on Site No. 2 and 5 computers on Site No. 3 as shown in enclosed plan layout.
- The servers (one main and one backup server), hubs, firewall, etc. are on Site No. 2 (second floor) with necessary cooling facilities and security features.
- We have decided to leave the 2Mbps leased line as it is, as it would work out cheaper for the computer which they use the Internet all the time.
- The server is combined of the print server, database server and a file server.
- The staff who is currently using Linux will have to be trained to use the Windows NT.
- The used Network cards are compatible to the existing new topologies.
- I have designed a flexibility system for the company which it will give room for it to grow in the future.
- TCP/IP protocols are already installed in the applications.

UTP (CAT 5) 10/100BASE-T ETHERNET CABLE

The cables are an absolutely necessary part of any network and they can give a real importance to the cost of the whole system. Cabling means that the computers are linked together. There are many type of cables and they are the following:

- Fibre Optic cable
- Coaxial cable
- Shielded twisted pair wire
- Unshielded twisted pair wire

I have choose this Ethernet Cable because it save me from buying separate connectors to make a cable which is costing time and money for this company, as it very simply to connect (to other devices requiring a RJ-45 (100Base TX) type Connector.

The 100 Base TX uses a star topology in which each node connects to a central contractor or a multiport repeater.

LAN

In this assignment, I have decided to use the ring topology. Even though it is more expensive than the bus topology, it is more quickly and efficient and less prone to collisions. I'm used 16Mbps of LAN.

Intel Express 330T 24 port Stackable Dual Speed Hub w/ 24x RJ-45 ports

Hubs or concentrators are hardware devices, which it enables LANs to be linked to each other and to WANs. The ring or bus topologies of a LAN can be connected to the backbone of a WAN.

I have decided to have 2 x Intel Express 330T 24 port Stackable Dual Speed Hub, having 48 x RJ-45 Connector type ports altogether, leaving out 5 ports (43 ports are used by 37 computers and 5 printers and 1 backup server) left for expansion to connect more computers or more hubs when required in the future.

I choose this Intel Express 330T 24 port Stackable Dual Speed Hub because it is very useful for connecting all 24 (or less) devices at once, for example, when you have 12 computers, 5 printers and 1 server, you can connect all 18 devices together into one 24 port hub and you still have 6 ports left over, instead of using 2 x 16 port hubs. You can stack more hubs onto the other if needed, saving some room (avoiding to spread them out around the whole place to waste space), very easy to install them and easy to use as well. Also, it can be running at 100Mb with downward capability with to 10Mb.

Firewall

A firewall is a system which it enforces an access control policy between two networks. The purpose of a firewall is to keep the intruders out the system while still letting one to carry on with their job in order to get it done.

Network Operating System

I have choose this Network Operating System because I think that is the most powerful operating system for business computing and it is very suitable for a large network of computers.

Also, why I choose this Network Operating System out of the other two operating systems (as shown below) because it is flexibility adaptability and reliability as mention as above and the fact is that both Windows NT Server and Windows NT Workstation are used mostly around the computing environment, even some companies use them for their network.

Linux Windows Vs NT Workstation

Linus Torvalds originally developed Linux as a hobby project at the University of Helsinki in Finland, with the help of many UNIX programmers and wizards across the Internet. The Linux kernel uses no code from AT&T or any other proprietary source, and much of the software available for Linux was developed by the GNU project of the Free Software Foundation in Cambridge, Massachusetts, U.S.A. However, programmers from all over the world have contributed to the growing pool of Linux software.

Linux is very old operating system which it goes back around 30 years and people are more user friendly with Microsoft Windows NT and Linux is more text based and command language, similar to DOS. People has to be special trained to use Linux operating system which they are not familiar with and that can cost time and money for this company whereas with Windows, people has a basic knowledge of Windows.

Windows 95 Vs Windows NT Workstation

The company called Microsoft in around 1996 launched it. This Operating System (OS) was written with a use of networks. The basic network paradigm is that of a Workgroup, a collection of peer PCs connected to a common LAN and using the same base communication protocol. Note that Windows 95 is a 32-bit multitasking system, and programs designed to use this capability will run much faster than an earlier version of Windows e.g. DOS (Disk Operating System) and Windows 3.1, Windows 3.11 for Workgroups, etc.

Windows 95 Vs Windows NT Workstation (continued)

Both Windows NT and Windows 95 have a similar Windows screen looks, provides much more interconnectivity between Windows programs and it allows you to safety keep more programs open than Windows 3.1. And both Windows NT and Windows 95 have been designed to run much faster than an earlier versions of Windows but in the end, when it comes to Networks, Windows NT is much better because it is specially designed for Networking and Windows 95 is out of date which it has to updated to the latest version which is Windows ME.

Security

The chance of security can be ending up with serious problems will be greater when working (using) with networks as the data or information is being passed around to and from many people and computer terminals. Also, if a virus does to able to manage to get into one node, it will then travels throughout the whole system and it will affect all the other computer terminals.

Forced Recognition Of Security

Forced recognition of security is are used to make sure that the users to know the importance of the security, for example, when an employee signs a contract which it states as a non-disclosure clauses which it means that, either he or she can be dismissed from employment in which they are been working in if they break any contract conditions including communicating with any confidential information to the next person or the other people.

Physical Access

Physical controls is when someone is not allowed to get near to the computer, or even not to close enough to switch the computer on and start to use it. It can be done in a number of ways, one of them is to not allow anyone controlling the access to the room with the computers are inside the room, it may be worked with a aid of keypads or any other special cards (i.e. identity cards, etc.) as an example. Another one is not to allow the wrong people access which it could be guards or plastic pass cards that it is being used to control access to the whole building. And the last one is locks on the computers can be used to not allow anybody without a proper access to turn the computers on, or simply just locking the computers away when the computers are not being used after hours or at night before leaving.

Logical Access

Logical control is used for controlling what the user has access to which it help to prevent a user or anyone from accessing, editing or damaging the most important information or data (the information is can be valuable) when they are not allowed to. There are two main types of network security and they are user level security and share level security. In user level security, the user must enter their user name (either he or she) and their password and the both of them must be correct before they are being able to log on to the network. Share level security are strict in a way, which it means that every single resource available on the network must have a password in order to be entered in so that, it allows to be able to have access to it.

The Data Protection Act 1984

The Data Protection Act was made in 1984 which it is only applies to automatically processed information (i.e. not information in paper files) which it relates to living individuals. For example, it does not cover information which it is relates only to a company or organisation and not to an individual. Organisation who are holding data relating to living individuals must register with the Data Protection Registrar, and must follow to the principles (as shown below), or they may be prosecuted. There may be a fee for the release of the information.

The data protection principles

1) Data shall be obtained fairly and lawfully.
2) Data shall only be held for specific purposes.
3) Data shall not be used in a compatible manner.
4) Data shall not be excessive to those purposes.
5) Personal data must be accurate and up to date.
6) Data shall not be entitled to have access to their data and where appropriate corrected.
7) Individuals shall be entitled to have access to their data and where appropriate corrected.
8) Appropriate security measures shall be taken to guard against unauthorised access or alteration.

Access rights

The access rights allows users to set rights to their directories, subdirectories and even individual files and it is possible to assign certain users read-only status, which it means that they can view the contents of the file but do not make any changes to the file. By the way the access rights are have been given mostly by the Local Area Network (LAN) software.

Copyright

The Copyright is a law against other people from copying the material which it is protected by copyright. Also it make sure that the creators of a software package or database are protected by copyright.

Software piracy

Software piracy involves the illegal copying of computing software and that is the same as software theft. If a company has a produced new software which it has developed by the software programmers (software developers), then all the money and time will be spent to produce a new software. Unfortunately for software developers, when people steal or copy and deal out software to other people instead of buying it, some of the people make extra copies of the software for sale. But if the people keep doing that, the software developers will end up loosing a lot of money.

Copyright of data

The data that it has first produced and it protected by copyright. For example of this, if the producer has published the data, which it has, been protected by copyright to stop the other publishers from re-producing.

The copyright, Designs and Patents Act 1988

It is a criminal offence if got caught by copying or stealing software, or any manuals which it comes with the software package(s) without any permission from the copyright owner or a licence from the copyright owner, and that is the person who is the software developer. It is offence There is a act which it makes it illegal to the organisation which they encourage to copy or deal out copies of illegal software and that is called The copyright, Design and Patents Act 1988.

Virus checking

What is a virus?

A virus is a small program designed to hide itself on to the computer. It cannot do physical damage, but it can give instructions to the computer to do anything from displaying an unwanted message to totally wiping out your hard disk. A virus can be built into an otherwise innocuous program, or it can hide itself away on a floppy disk. It is called a virus because, like a real virus in the body, it has the ability to replicate and press itself on. It does this by copying itself on to the hard disk and then back to any floppy disk put into the computer, so that it can go to infect another computer.

How to protect against a virus

The best way to solve a virus problem is not to catch one in the first place. The most common way of catching a virus is from a floppy disk made on another home or office computer. Where possible, try to avoid using disks copied from the other computers. You should also consider investing in virus-checking software e.g. Norton AntiVirus, etc. that will spot a virus and chase it out of your system. When you first put a copied disk in your computer, you must run the virus checker before doing anything. Prevention is better than cure.

Back-up procedures

Back-up is involved of the creation of copies of everything including the programs and data so that should the programs or data be lost, they are can be recreated at any time using the back-up copies. It is the best way to protect against disasters such as a disk failing, a file being erased, or even your computer is being stolen. The problem with backing up, and the reason that few people bother, is that you tend to need hundreds of floppy disks and it takes hours of work. But there is an alternative that doesn't take so long and protects you against the effects of losing a hard disk. Note that back-up copies are should be kept on a separate disk or tape and stored away from the computer system otherwise that the back-up copy may be get damaged. If a backup copy were kept on the same disk as the original, then if this disk were stolen or destroyed by fire the back-up copy would also be lost.

There are rules for backing up and they are the following:

- Try not to keep the back-up disk near the computer. What happens if the computer is stolen, the thieves will probably steal the disks as well. Also, ever, ever, try not to keep the back-up disk(s) in the drawer of the desk because this is where the first place will the thieves look.

- If you are holding a awful lot of data it would be very expensive to recreate, and it will take a really long time to re-enter all that information then you should invest in a fire/burglary safe to protect your back-ups from heat, theft, dust, humidity and damage.

Forced recognition of security

Information Technology have used forced recognition of security for different types of tasks, and that is including the operating nuclear power stations, and storing and updating medical records, insurance records and even police records. It is very important so that the security systems are in place to protect the system from deliberate or accidental harm with awful lot of information being held around.

Non-disclosure agreements

Non-disclosure agreements are placed in a contract of the employment to on employees when they are no more working in an organisation. Sometimes nondisclosure agreements are used to prevent the person from speaking about their previous employment.

Official Secrets Act

This act was used to protect the privacy of information, which the Crown holds it, and to protect national security. Some of the people have to sign the official Secrets Act as a condition of their employment that is including prison warden, police officers etc.